Securing the Internet

Digital Signatures & Electronic Transactions in California

Prepared by
The California State Assembly
Committee on Information Technology

The Honorable John A. Dutra, Chair

July 24, 2000
State Capitol
Sacramento, California

Securing the Internet

Digital Signatures & Electronic Transactions in California

Prepared by
The California State Assembly
Committee on Information Technology

The Honorable John A. Dutra, Chair

August 2, 2000
State Capitol, Sacramento, California

Table of Contents

Executive Summary

California adopted the Digital Signature Act in 1995. However, according to the Secretary of State, five years later and despite the adoption of a comprehensive regulatory scheme not one state agency in California is currently using digital signatures in any of its transactions.

The "non-use" of digital signatures in the State of California may very well stem from concerns that citizens and consumers continue to entertain regarding the security of transactions that involve the Internet. However, digital signatures are purported to be even more secure than manual, written signatures.

Indeed, surveys of private sector activity have suggested that consumers' concerns regarding internet security have less to do with electronic transactions themselves than with the methods in which online merchants handle their personal information after the consumer submits it to them over the Internet. It has been suggested that security concerns regarding Internet transactions that involve digital signatures may be alleviated with the use of third party authentication services and education about how these authentication services work.

The California Legislature has been at the forefront of the e-commerce movement with the passage of two primary pieces of legislation: the California Uniform Electronic Transactions Act, or "UETA," and the California Digital Signature Act of 1995

California UETA declares that all electronic transactions should be given the same legal effect as transactions that are recorded on paper and that an electronic signature cannot be denied its legal effect solely because it is in electronic form.

California's Digital Signature Act of 1995 creates a criteria-based approach to dealing with digital signatures. In order for a digital signature to be valid, it must: be unique to the person using it, be capable of verification; under the sole control of the person using it; linked to the data in such a manner that if the data is changed, the signature is invalidated; and conform with regulations adopted by the Secretary of State.

These regulations, subsequently adopted by the Secretary of State, require that in order for a digital signature to be valid, a form of technology that has been approved by the Secretary of State must create it. Currently, the Secretary of State has authorized that digital signatures created by the Public Key Infrastructure or "PKI" and Signature Dynamics technologies are to be given their full legal effect because they meet all of the enumerated requirements of the Digital Signature Act.

Currently, the Office of the Secretary of State is unaware of any state agency that is using or in the process of developing digital signature technology. The office fears that digital signatures suffer from a "chicken and egg" problem. Agencies are weary of creating digital signature technology until citizens have acquired digital signatures. However, citizens are unwilling to acquire digital signatures until agencies have developed applications for digital signature usage.

Concerns, regarding the transmission of information over the Internet to state agencies, most likely stem from the public's unfamiliarity with available technology and have little to do with the actual quality of security offered by digital signatures. Additionally, many of the concerns that citizens entertain regarding these transactions may have more to do with a lack of notice regarding the privacy and security of the websites these transactions take place on.

As implementation of digital signatures is still in the infancy stage, numerous actions in the Legislature may still be taken in order to effectively promote secure e-commerce and "government-to-citizen" Internet transactions through the use of digital signatures. The effect, if any, of the recent enactment of a federal digital signature law on the state's own digital signature law and UETA may prompt further re-examination. In addition, California must define the rules of conduct applicable to the use of digital signatures by individuals and create standard incentives for state agencies to better integrate digital signature technology into Internet-based initiatives.

Internet Transaction Security Concerns Persist

Digital signatures, if created by the appropriate technology, are convenient, low-cost, and more secure than manual, written signatures. For all practical purposes, digital signature software is so good that these signatures are virtually “forge-proof.”[1]

However, the public’s distrust of Internet transactions persists, and has been well documented by the media. The most plausible reason for the public’s distrust of the security of many transactions is that the public is unfamiliar with the high level of security offered by digital signature technology. Additionally, the media’s constant portrayal of “hackers’ exploits” and the federal government’s stance towards encryption export controls do not aid in the public’s trust of digital signatures.[2]

Recent research has documented that consumers regard most websites as having a low regard for consumer protection.[3] Consumers fear that hackers will gain access to their personal information and use it against them. However, after filtering through the abundance of research that exists regarding the consumers’ distrust of Internet transactions, it is apparent that many of their concerns have little to do with the security of the transactions themselves. For example, most consumers are concerned with how the company they submit their information to will use the information once it is in their possession.[4]

[1] Mark Grossman, *Contracts Using Digital Signatures (Part II)* (visited July 14, 2000) <www.mgrossmanlaw.com/articles/1996/contracts_using_digital_signatur.htm>.

[2] John Cunningham, Esq., *Paperless Real Estate Transacrions—How Far Behind Can We Be?* (visited June 7, 2000) <www.eatonpeabody.com/art_paperless.htm> (copy on file with the California Assembly Committee on Information Technology).

[3] Cheskin Research, Trust in the Wired Americas (July 2000).

[4] *Id.*

In most digital signature situations, the primary threat to the validity of the transaction is fraud — parties to the transaction want to make sure that the person who created the signature is really who they say they are. In cases where the digital signature is created through Public Key Infrastructure technology, third party certification authorities will verify that the individual to the transaction is who he or she is.

If an instance of fraud occurs, certification authorities, like Verisign, Inc., of Mountain View, California, have insurance programs that can be purchased that limit the digital certificate holder’s liability if their digital signature is compromised.

Additionally, certification authorities can easily be prevented from releasing personal information about the digital signature user through tort or contract law. These authorities are independent entities, consumers do not need to worry about government accessing their personal information contained in an authority’s depository.

The Internet and Need for Secure Transactions

The Internet’s predecessors, including the federal Advanced Research Project Agency Network, or ARPANET, and the National Science Foundation's NSFNET, began to develop in the 1970s and 1980s, the population of users was limited to government, defense, education and research agencies. However, in the early 1990s, as the Internet grew and evolved, the population of Internet users grew tremendously. Today, commercial facilities, private individuals, government organizations, and researchers all over the world use the Internet.

With the expansion in the user base of the Internet also came an increase in the number of commercial transactions taking place electronically. This rise of e-commerce has facilitated and, in many respects, demanded the development of a secure contracting standard for transactions that take place over the Internet. However, the law, in many situations, requires a written manual signature in many transactions in order to authenticate the transaction.

With the emergence of electronic transactions, it quickly became apparent that a manual signature would not always be available or viable. The lack of a secure, legal digital signature law has caused many consumers, companies and governments to be weary of the potential for fraud in electronic transactions. Subsequently, many state Legislatures and Congress have focused their efforts on developing ways to authenticate electronic and digital signatures and facilitate transactions that are both secure and enforceable.

The California Uniform Electronic Transactions Act

In order to bring some uniformity to the world of electronic transactions, in 1999, the National Conference of Commissioners on Uniform State Laws (NCCUSL) developed the Uniform Electronic Transactions Act, or “UETA,” in 1999. UETA represented the first “national effort at providing some uniform rules to govern transactions in electronic commerce that should serve in every state.”[5]

It is intended that state legislatures which enact UETA will be ensuring that electronic transactions are just as enforceable as transactions recorded

[5] National Conference Commissioners on Uniform State Laws, *Summary: Uniform Electronic Transactions Act* (visited May 23, 2000) <www.nccusl.org/uniformact_summaries/uniformacts-s-ueta.htm>.

with manual signatures, without creating an entirely new and unique legal standard that only applies to electronic transactions.

Indeed, the basic objective of UETA is to ensure "that an electronic record of a transaction is the equivalent of a paper record, and that an electronic signature will be given the same legal effect, whatever that might be, as a manual signature [in order to] remove perceived barriers to electronic commerce."[6]

Of course, states, if interested, are free to adopt the UETA as developed by the NCCUSL, they may develop their own rules governing electronic transactions, or they may simply choose not to act. At the time of this report, 13 states, including California, have adopted variations of the UETA and 15 states have introduced legislation resembling the UETA.

Legislatures adopting UETA have recognized that state governments need to set standards to make contracts and commitments enforceable regardless of the physical nature of the signature affixed to the contract. In enacting various versions of the UETA, states have been particularly concerned about the effect that electronic transactions will have on traditional legal writing and signature requirements.

In September 1999, Governor Davis signed SB 820 (Sher) (Chapter 428, Statutes of 1999) enacting the California Uniform Electronic Transactions Act. SB 820 largely followed UETA as drafted by NCCUSL; however, some amendments were made to the California version including the exemption of a number of state laws. These exemptions include the following:

(1) "All statutes which require specifically identifiable text or disclosures in a record or a portion of a record be separately signed or initialed."

[6] *Id.*

(2) "Statutes with special notice requirements or where the notices trigger particular legal rights such as the running of a time period to appeal."
(3) "Statutes affecting post-contract rights or activities."
(4) "Statutes which were passed to restrain particular types of activities."[7]

As NCCUSL intended, SB 820 promulgates the goal that electronic transactions should be given the same legal effect as transactions that are recorded on paper by providing that a record, contract, or signature can not be denied its legal effect solely because it is electronic in nature. It is generally accepted that the Act provides Californians and California businesses with a uniform set of rules governing electronic transactions and should play a positive role in promoting the secure growth of e-commerce.

Enactment of the Federal Digital Signatures Bill

On June 30, 2000 President Clinton signed the Electronic Signatures in Global and National Commerce Act into law creating a national framework for interstate and foreign electronic transactions. According to the Information Technology Association of America (ITAA), the Act achieves four notable goals:

(1) "Its broad pre-emption language creates a uniform national standard for the validity of online contracts, avoiding the potential of a patch quilt of differing state-based approaches;"
(2) "It proves for the validity of transferable records executed using an online process;"
(3) "It creates important protections and safeguards for consumers necessary to instill confidence in the full promise of e-commerce;" and
(4) "The statute codifies the principle of technical neutrality—Congress and the states will not legislate or ordain the evolution of new technologies in this space."[8]

[7] CAL. CIV. CODE § 1633.1 (enacted by Chapter 428).

The Electronic Signatures in Global and National Commerce Act urges states to adopt the Uniform Electronic Transactions Act, which California has already done. The adoption of UETA, consistent with the Electronic Signatures Act clarifies the scope of interstate commerce as it applies to Internet transactions.

The Electronic Signatures in Global and National Commerce Act affects those transactions that deal with interstate or foreign commerce, pre-empting individual state laws that touch on the same matter. In addition, because of the *Act's* pre-emptive qualities, states are severely limited in their ability to create digital signature legislation regulating the enforceability of contracts. This leaves states essentially three options. They can either create their own legislation for intrastate commerce, enact UETA, or simply accept the pre-emption of the federal legislation.

If states, like California, choose to limit the scope of their electronic transactions law to apply only to intrastate commerce, the outcome is unclear. Large amounts of satellite litigation regarding the definition of intrastate commerce may overburden state court dockets. In addition, the question persists of whether any Internet transaction can be defined as solely an intrastate transaction. The Federal Communications Commission, for example, has ruled that ISP's and the Internet itself are subject to their jurisdiction under the Federal Communications Acts of 1934 and 1996."[9]

[8] Information Technology Association of America, *Digital Signature Legislation S. 761: Summary and Analysis* (2000).

[9] *Id.*

California's Digital Signature Statute and Regulations

The California Legislature had its eye on the electronic transaction arena in 1995, long before it enacted the California Uniform Electronic Transaction Act. The Digital Signature Act of 1995 provides that if a state department so chooses, some or all of the communications with that department may be conducted electronically.

The Legislature, in enacting the Digital Signature Act, elected to adopt a criteria-based approach to digital signatures and directed the Secretary of State to develop regulations for its implementation. It was further the state's goal to promote the expansion of digital signatures by avoiding strict statutory requirements that could stifle the introduction of new digital signature technologies as they are developed.

The criteria established by the Digital Signature Act of 1995 provides, "[a]n electronic signature is legally effective if it is:

a. Unique to the person using it;
b. Capable of verification;
c. Under the sole control of the person using it;
d. Linked to the data in such a manner that if the data is changed the signature is invalidated; and
e. In conformity with regulations adopted by the appropriate state agency usually the Secretary of State."[10]

The Act and its associated regulations have established the appropriate measures to insure against fraudulently created signatures. The "unique" and "verification" requirements established by the Act are critical to assuring the identity and validity of any electronic transaction. Additionally, AB 1577 provided that a digital signature is only valid if the signature is "linked to the data in such a way that it is invalidated if the data is changed."

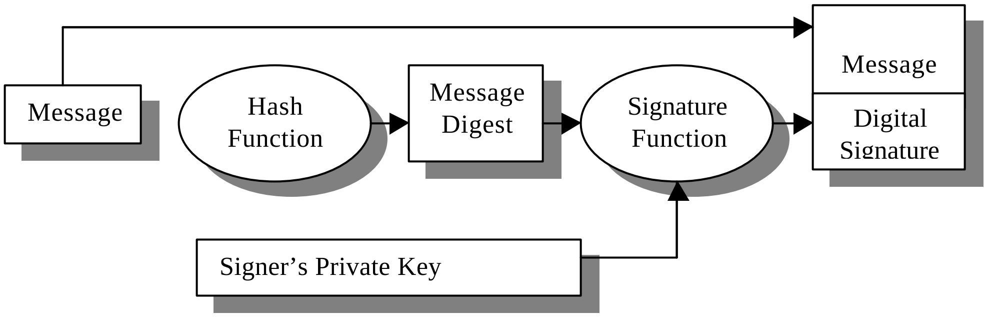
[10] CAL. CIV. CODE § 1633.1 (enacted by Chapter 428).

Digital Signature Regulations & Technology

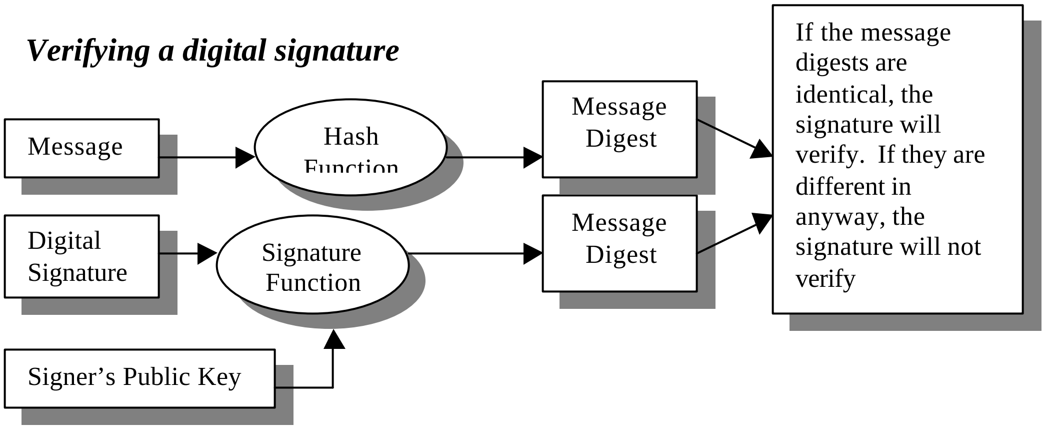
The Secretary of State, presently, has authorized that digital signatures created by the Public Key Infrastructure, or “PKI,” and Signature Dynamics technologies, which meet established statutory requirements, are to be given their full legal effect.

- California Code of Regulations § 22000 provides that a digitally signed communication “is a message that has been processed by a computer in such a manner that ties the message to the individual that signed the message.”
- California Code of Regulations § 22001 provides that a digital signature must be created by a form of technology that has been accepted by the State of California in order for the digital signature to be valid.
- California Code of Regulations § 22002 outlines the requisite criteria to be met in order for the digital signature to be legally effective.
- California Code of Regulations § 22003 provides that Public Key Infrastructure is an acceptable method of creating a valid, legally binding digital signature.
- California Code of Regulations § 22004 outlines the process by which a company or individual can apply to add a new technology to the Secretary of State’s list of acceptable digital signature technologies.
- California Code of Regulations § 22005 requires public entities that use digital signatures to ensure that the digital signature is sufficiently secure.

Creating a digital signature



Verifying a digital signature


Message
Hash Function
Message Digest
Digital Signature
Signature Function
Message Digest
Signer's Public Key
If the message digests are identical, the signature will verify. If they are different in anyway, the signature will not verify

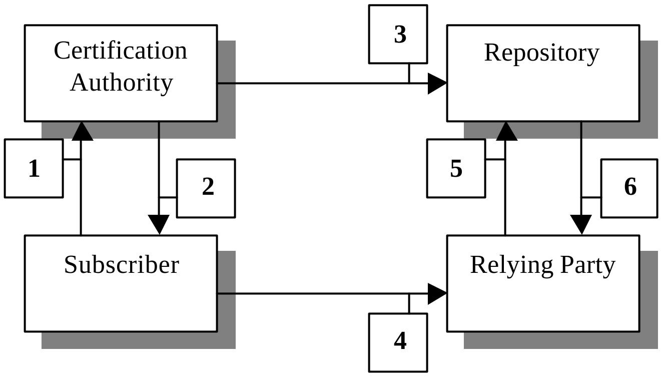
Diagrams provided by Digital Signature Trust Co., www.digsigtrustco.com/digital/signatures.html

Public Key Infrastructure allows a person wishing to use a digital signature to create two encryption keys. "The first key, the private key, is kept secret, and is used to encrypt the message. The second key, the public key, is used to decrypt the message."[11] The person who creates the message retains the private key and the public key is distributed to those who are the intended recipients of the message.

[11] Department of Financial Institutions, *Commissioner's Comments: Electronic Commerce and Financial Services Regulatory Challenges* (visited May 15, 2000) <www.dfi.ca.gov/newsltr/spring99/1999.htm>.

Since only the private key can encrypt the message, or lock it, the recipient of the message, who decrypts or unlocks the message, with the digital signature affixed, can be sure that the message was actually sent by sender. A PKI system assures the recipient that the sender created the public key by allowing for automatic verification of the sender's identity through the use of a Certification Authority. A Certification Authority is a third party to the transaction that verifies the identity of the sender of the message before the keys are created.

PKI Process Flow



Step 1: Subscriber applies to Certification Authority for Digital Certificate.
Step 2: CA verifies identity of Subscriber and issues Digital Certificate.
Step 3: CA publishes certificate to Repository.
Step 4: Subscriber digitally signs electronic message with Private Key to ensure Sender Authenticity, Message Integrity and Non-Repudiation and sends to Relying Party.
Step 5: Relying Party receives message, verifies Digital Signature with Subscriber's Public Key, and goes to Repository to check status and validity of Subscriber's Certificate.
Step 6: Repository returns results of status check on Subscriber's Certificate to Relying party.

Diagram provided by Digital Signature Trust Co.,
www.digsigtrustco.com/digital/signatures.html

In California, any agency that chooses to use PKI technology must use a Certification Authority that is registered with the Secretary of State. In order for a Certification Authority to become registered with the Secretary of State it must undergo an audit conducted by a third-party corporation authorized to conduct financial investigations. Currently, only two Certification Authorities are registered with the Secretary of State: Verisign, Inc. of Mountain View, California and Digital Signature Trust Co. of Salt Lake City, Utah.

A state agency can also use digital signatures created by Signature Dynamics or "SD" technology. "Signature Dynamics uses a digitized version of the sender's physical signature. The person sending the message literally signs his or her name on a pad which digitally records the speed, pressure, and emphasis of that signature."[12] A digest of the signature is created and run through a "hash" program which encrypts the digest. The encrypted signature is then electronically attached to the message. However, if any portion of the message is altered or tampered with in any manner, the signature becomes invalidated.

Unlike PKI technology that employs the use of Certification Authorities, digital signatures created by SD are not capable of immediate authentication. However, a confirmation of the signature can be made at anytime after the message has been received.

Unfortunately, because the Secretary of State does not keep statistics regarding state agencies that choose to use digital signatures, there is no precise data regarding the use of digital signatures in the state. However, at this time, the Secretary of State's office is unaware of any state agency that it is employing the use of digital signatures.

[12] *Id.*

The Office of the Secretary of State, has further surmised that widespread use of digital signatures in state agencies has been slow because of a “chicken and the egg” implementation problem. Agencies are weary of creating digital signature applications until people have acquired digital signatures. However, people are unwilling to acquire digital signatures until agencies have created applications that require the use of digital signature technology.

The Future of Digital Signature Law

To effectively promote electronic commerce through the use of digital signatures, the law must accomplish two primary goals. First, California must effectively promote the use of digital signatures by state agencies when implementing programs and projects on the Internet. Second, California must define the scope of its own UETA law—either by further defining the scope of existing state law or allowing federal law to pre-empt state law.

This is a multi-faceted project. The first step is to educate the public about digital signatures and to gain the public’s trust and confidence in electronic transactions. Studies show that public trust of electronic transactions increases with experience. This means that California needs to begin putting digital signatures to use in California so the public can acquire them and begin to use them in electronic transactions.

In order to balance the use of digital signatures with the public’s concern about Internet security, when digital signature use is introduced policymakers should take the opportunity to look into instances of fraud and other privacy and identity theft related issues.

The Legislature must define the rules of conduct that are to apply to electronic transactions and digital signatures. If the body of law that is to apply to electronic transactions can be effectively defined, this will aid in creating predictability and consistency in electronic transactions which can eventually evolve into increased public confidence of electronic transactions. Should the Legislature wait too long to define the controlling body of laws, this decision may be left up to the judicial system and it could take years for courts to define the body of laws that govern electronic transactions for years to come.

Appendices

1. Consumer's Union, *Uniform Electronic Transactions Act: Consumer Nightmare or Opportunity?*, <www.consumersunion.org/finance/899nclcwc.htm>.

2. National Conference of Commissioners on Uniform State Laws, *Summary: Uniform Electronic Transactions Act*, <www.nccusl.org/uniformact_summaries/uniformacts-s-ueta.htm>.

3. National Conference of Commissioners on Uniform State Laws, *A Few Facts About the Uniform Electronic Transactions Act*, <www.nccusl.org/uniformact_factsheets/uniformacts-fs-ueta.htm>.

4. National Conference of Commissioners on Uniform State Laws, *Why States Should Adopt the Uniform Electronic Transactions Act*, <www.nccusl.org.org/uniformact_why/uniformacts-why-ueta.htm>.

5. Senate Bill 820 (Statutes of 1999, Chapter 428).

6. Consumers Union, *California Exemptions to UETA*, <www.consumersunion.org/finance/9991wc00.htm>.

7. Information Technology of America, *Digital Signature Legislation S. 761: Summary and Analysis*.

8. Electronic Signatures in Global and National Commerce Act S. 761.

9. California Secretary of State, *Secretary of State Jones Brings Widespread Expansion of E-Government One Step Closer to Reality*, <www.ss.ca.gov/digsig/press1014.htm>.

10. California Secretary of State, *Secretary of State Jones Pro[poses Regulations to Allow Digital Signatures to be Used by Public Entities in California*, <www.ss.ca.gov/digsig/press.htm>.

11. California Secretary of State, *Jones Approves Second Company to Provide Digital Signature Services to State and Local Government in California*, <www.ss.ca.gov/digsig/press1118.htm>.

12. Assembly Bill 1577 (Statutes of 1995, Chapter 594).

13. CAL. GOV. CODE § 16.5 (enacted by Chapter 594).

14. C.C.R. § 22000 et. seq.

15. California Secretary of State, *Approved List of Digital Signature Certification Authorities*, <www.ss.ca.govdigsig/cert1.htm>.

16. California Secretary of State, *Frequently Asked Questions About California's Digital Signature Law and Regulations*, <www.ss.ca.gov/digsig/digsigfaq.htm>.

17. Mark Grossman, *Computer Law Tip of the Week: Contracts Using Digital Signatures (Part II)*, <<ww.mgrossmanlaw.com/articles/1996/contracts_using_digital_signatur.htm>>.

18. Walter J. Mix, *Commissioner's Comments: Electronic Commerce and Financial Services Regulatory Challenges*, The State Charter <www.dfi.ca.gov/newsltr/spring99/1999.htm>.

19. Internet Law and Policy Forum, *Survey of State Electronic & Digital Signature Legislative Initiatives*, <www.ilpf.org/digsig/digrep/htm>.

20. Digital Signature Trust Co., *Digital Signatures and Public Key Infrastructure (PKI) 101*, <<www.digsigtrust.com/pdsb.html>.

21. John A. Cunningham, *Paperless Real Estate Transactions—How Far Behind Can We Be?*¸Eaton, Peabody, Bradford, & Veague <www.eatonpeabody.com/art_paperless.htm>.

22. C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, <www.w3journal.com/7/s3.biddle.wrap.html>.

23. Cheskin Research, *Trust in the Wired Americas*, July 2000.